



# UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/461,984	12/15/1999	JIN LU	PHA-23-890	4517

24737 7590 08/16/2005

PHILIPS INTELLECTUAL PROPERTY & STANDARDS  
P.O. BOX 3001  
BRIARCLIFF MANOR, NY 10510

EXAMINER

HOFFMAN, BRANDON S

ART UNIT	PAPER NUMBER
----------	--------------

2136

DATE MAILED: 08/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

09/461,984

Applicant(s)

LU ET AL.

Examiner

Brandon S. Hoffman

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 27 June 2005.  
2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.  
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-29 is/are pending in the application.  
4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.  
6) ☒ Claim(s) 1-29 is/are rejected.  
7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.  
8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.  
10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some \* c) ☐ None of:  
1. ☐ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)  
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)  
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.  
4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_.  
5) ☐ Notice of Informal Patent Application (PTO-152)  
6) ☐ Other: \_\_\_\_\_

### DETAILED ACTION

1. Claims 1-29 are pending in this office action, claims 24-29 are newly added.
2. Applicant's arguments, filed June 27, 2005, have been fully considered but they are not persuasive.

### *Rejections*

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

### ***Claim Rejections - 35 USC § 103***

4. Claims 1-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kim et al. (U.S. Patent No. 5,799,081) in view of Zhang et al. (U.S. Patent No. 6,550,008), and further in view of International Telecommunication Union, hereinafter referred to as ITU-T.

Regarding claim 1, Kim et al. teaches a system for copy protecting information, the system comprising:

- A point of deployment module (fig. 4, ref. num 22); and
- A set-top box including (fig. 4, ref. num 20);

- Wherein the set-top box transmits a request message for information (fig. 21, host device transfers EMM, ECM, and CPTC to smart card),
- The point of deployment module generates a reply message (fig. 21, smart card responds by sending CW),
- The reply message including at least one control information pair,
  - Each pair having copy control information and a stream identifier (col. 18, lines 46-48) and
- Generating a first key in the point of deployment module, using the at least one control information pair (fig. 21, CW created in deployment module from EMM, ECM, and CPTC).

Kim et al. does not specifically teach the control information pair includes a stream identifier, generating a second key in the set-top box, the point of deployment module encrypting the information with the first shared key and transmitting the encrypted information to the set-top box, and the set-top box decrypting the encrypted information with the second shared key when the first and second shared keys match.

Zhang et al. teaches generating a second key in the set-top box (col. 10, lines 10-17), the point of deployment module encrypting the information with the first shared key and transmitting the encrypted information to the set-top box (col. 10, lines 22-25), and the set-top box decrypting the encrypted information with the second shared key when the first and second shared keys match (col. 10, lines 25-29).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine generating a second key in the set-top box, the POD encrypting the information with the first shared key and transmitting the information to the set-top box, and the set-top box decrypting the information when the keys match, as taught by Zhang et al., with the system of Kim et al. It would have been obvious for such modifications because shared session keys, used for symmetric key cryptosystems, provide authentication of devices as well as keeping data secure.

Kim et al. as modified by Zhang et al. still does not teach the control information pair includes a stream identifier.

ITU-T teaches the control information pair includes a stream identifier (fig. F.7).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the control information pair including a stream identifier, as taught by ITU-T, with the system of Kim et al. as modified by Zhang et al. It would have been obvious for such modifications because a stream identifier would identify the elementary stream, e.g., data files. This is similar to how ECM contains a content identifier to correctly identify the content in which it refers to. The teachings of Kim et al. use ECM to identify the content, which can be transferred together with the CPTC (see col. 18, lines 61-67 of Kim et al.).

Regarding claim 2, Kim et al. teaches a method of copy protecting information transmitted between a deployment module and a host device, the method comprising the steps of:

- Transmitting a request message for the information from the host device to the deployment module (fig. 21, host device transfers EMM, ECM, and CPTC to smart card);
- Transmitting a reply message from the deployment module to the host device (fig. 21, smart card responds by sending CW),
- Wherein the reply message includes at least one control information pair,
  - Each pair having copy control information and a stream identifier (col. 18, lines 46-48) and;
- Generating a second shared key at the deployment module, using the at least one control information pair and an encryption means (fig. 21, CW created in deployment module from EMM, ECM, and CPTC);
- Decrypting, at the host, the encrypted information (fig. 21, ref. num 263 uses CW to decrypt the information).

Kim et al. does not specifically teach the control information pair includes a stream identifier, encrypting, in the deployment module, the information, transmitting the encrypted information from the deployment module to the host, and receiving the information at the host when the first and second shared keys match.

Zhang et al. teaches generating a second key in the set-top box (col. 10, lines 10-17), the point of deployment module encrypting the information with the first shared key and transmitting the encrypted information to the set-top box (col. 10, lines 22-25), and the set-top box decrypting the encrypted information with the second shared key when the first and second shared keys match (col. 10, lines 25-29).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine generating a second key in the set-top box, the POD encrypting information with the first shared key and transmitting the information to the set-top box, and the set-top box decrypting the information with the second shared keys when they match, as taught by Zhang et al., with the system of Kim et al. It would have been obvious for such modifications because shared session keys, used for symmetric key cryptosystems, provide authentication of devices as well as keeping data secure.

Kim et al. as modified by Zhang et al. still does not teach the control information pair includes a stream identifier.

ITU-T teaches the control information pair includes a stream identifier (fig. F.7).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the control information pair including a stream

identifier, as taught by ITU-T, with the method of Kim et al. as modified by Zhang et al.

It would have been obvious for such modifications because a stream identifier would identify the elementary stream, e.g., data files. This is similar to how ECM contains a content identifier to correctly identify the content in which it refers to. The teachings of Kim et al. use ECM to identify the content, which can be transferred together with the CPTC (see col. 18, lines 61-67 of Kim et al.).

Regarding claim 3, the combination of Kim et al. as modified by Zhang et al./ITU-T teaches wherein the deployment module is a point of deployment module (see col. 3, line 16 of Zhang et al.).

Regarding claim 4, the combination of Kim et al. as modified by Zhang et al./ITU-T teaches wherein the host is a set-top box (see col. 1, line 28 of Zhang et al.).

Regarding claim 5, the combination of Kim et al. as modified by Zhang et al./ITU-T teaches wherein the encryption means includes a hash function (see col. 10, lines 36-39 of Zhang et al.).

Regarding claim 6, the combination of Kim et al. as modified by Zhang et al./ITU-T teaches wherein the encrypted information in an elementary stream of information is encrypted with the first shared key (see fig. 4, step num 9 of Zhang et al.).



Regarding claim 7, the combination of Kim et al. as modified by Zhang et al./ITU-T teaches wherein the stream identifier that is transmitted to the host is incorporated with the Packetized Elementary Stream (PES) header of the elementary stream (see page xi, section intro. 8.1 of ITU-T).

Regarding claim 8, Kim et al. teaches a deployment module for use with a host device, the deployment module comprising:

- Means for communicating with the host device (fig. 4, ref. num 23 and col. 2, lines 54-56); and
- A processor for (fig. 5, ref. num 39 and col. 3, lines 25-27),
  - In response to a request message for information from the host device, generating a reply message to the host device (fig. 21, host device transfers EMM, ECM, and CPTC to smart card in exchange for CW),
- The reply message including at least one control information pair,
  - Each pair having copy control information and a stream identifier (col. 18, lines 46-48),
- Generating a first shared key using the at least one control information pair (fig. 21, CW created in deployment module from EMM, ECM, and CPTC, i.e., the control information pair).

Kim et al. does not specifically teach the control information pair includes a stream identifier, the generating of a first key is for a shared key, and encrypting the

Art Unit: 2136

information with the first shared key and transmitting the encrypted information to the host device.

Zhang et al. teaches the generating of a first key is for a shared key (col. 10, lines 10-17), and encrypting the information with the first shared key and transmitting the encrypted information to the host device (col. 10, lines 22-25).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine generating a first shared key and encrypting the information with the first shared key and transmitting the encrypted information to the host device, as taught by Zhang et al., with the system of Kim et al. It would have been obvious for such modifications because shared session keys, used for symmetric key cryptosystems, provide authentication of devices as well as keeping data secure.

Kim et al. as modified by Zhang et al. still does not teach the control information pair includes a stream identifier.

ITU-T teaches the control information pair includes a stream identifier (fig. F.7).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the control information pair including a stream identifier, as taught by ITU-T, with the module of Kim et al. as modified by Zhang et al.

Art Unit: 2136

It would have been obvious for such modifications because a stream identifier would identify the elementary stream, e.g., data files. This is similar to how ECM contains a content identifier to correctly identify the content in which it refers to. The teachings of Kim et al. use ECM to identify the content, which can be transferred together with the CPTC (see col. 18, lines 61-67 of Kim et al.).

Regarding claims 9 and 14, the combination of Kim et al. as modified by Zhang et al./ITU-T teaches wherein the deployment module is selected from the group consisting of a point of deployment module, wireless data interface appliance, smartcard, personal computer, or Internet interface appliance (see col. 3, line 16 of Zhang et al.).

Regarding claims 10 and 15, the combination of Kim et al. as modified by Zhang et al./ITU-T teaches wherein the host is a set-top box (see col. 1, line 28 of Zhang et al.).

Regarding claims 11 and 16, the combination of Kim et al. as modified by Zhang et al./ITU-T teaches wherein the encrypted information is transmitted to the host device using a transport stream, wherein the transport stream includes at least one elementary stream (see col. 2, lines 57-59 of Kim et al.).

Regarding claims 12 and 17, the combination of Kim et al. as modified by Zhang et al./ITU-T teaches wherein respective ones of the at least one control information pairs is associated with respective ones of the at least one elementary streams (see Fig. F7 of ITU-T, an elementary stream is associated with control information pairs because each elementary stream requires a stream identifier).

Regarding claim 13, Kim et al. teaches a host device for use with a deployment module (fig. 7), the host device comprising:

- Means for communicating with the deployment module (fig. 4, ref. num 23); and
- A processor for (fig. 4, ref. num 27),
  - Generating a request message for information to the deployment module, and in response, receiving a reply message from the deployment module (fig. 21, host device transfers EMM, ECM, and CPTC to smart card in exchange for CW),
- Wherein the reply message including at least one control information pair,
  - Each pair having copy control information and a stream identifier (col. 18, lines 46-48),
- Decrypting encrypted information, received from the deployment module, with the second shared key (fig. 21, ref. num 263 uses CW to decrypt the information).

Kim et al. does not specifically teach the control information pair includes a stream identifier, generating a second shared key using the at least one control

Art Unit: 2136

information pair, and receiving the information when the second shared key matches a first shared key generated in the deployment module.

Zhang et al. teaches generating a second key in the set-top box (col. 10, lines 10-17), and receiving the information when the second shared key matches a first shared key generated in the deployment module (col. 10, lines 25-29).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine generating a second key in the set-top box and receiving the information when the shared keys match, as taught by Zhang et al., with the system of Kim et al. It would have been obvious for such modifications because shared session keys, used for symmetric key cryptosystems, provide authentication of devices as well as keeping data secure.

Kim et al. as modified by Zhang et al. still does not teach the control information pair includes a stream identifier.

ITU-T teaches the control information pair includes a stream identifier (fig. F.7).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the control information pair including a stream identifier, as taught by ITU-T, with the module of Kim et al. as modified by Zhang et al.

Art Unit: 2136

It would have been obvious for such modifications because a stream identifier would identify the elementary stream, e.g., data files. This is similar to how ECM contains a content identifier to correctly identify the content in which it refers to. The teachings of Kim et al. use ECM to identify the content, which can be transferred together with the CPTC (see col. 18, lines 61-67 of Kim et al.).

Regarding claim 18, Kim et al. teaches an article of manufacture comprising a computer readable medium in which resides a computer program, said article being part of a deployment module for use with a host device, said program comprising:

- Instruction means for communicating with the host device (fig. 4, ref. num 23 and col. 2, lines 54-56); and
- Instructions for, in response to a request for information from the host device, generating a reply message to the host device (fig. 21, host device transfers EMM, ECM, and CPTC to smart card in exchange for CW),
- The reply message including at least one control information pair, each pair having copy control information and a stream identifier (col. 18, lines 46-48),
- Generating a first shared key using the at least one control information pair (fig. 21, CW created in deployment module from EMM, ECM, and CPTC, i.e., the control information pair).

Kim et al. does not specifically teach the control information pair includes a stream identifier, the generating of a first key is for a shared key, and encrypting the

information with the first shared key and transmitting the encrypted information to the host device.

Zhang et al. teaches the generating of a first key is for a shared key (col. 10, lines 10-17), and encrypting the information with the first shared key and transmitting the encrypted information to the host device (col. 10, lines 22-25).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine generating a first shared key and encrypting the information with the first shared key and transmitting the encrypted information to the host device, as taught by Zhang et al., with the system of Kim et al. It would have been obvious for such modifications because shared session keys, used for symmetric key cryptosystems, provide authentication of devices as well as keeping data secure.

Kim et al. as modified by Zhang et al. still does not teach the control information pair includes a stream identifier.

ITU-T teaches the control information pair includes a stream identifier (fig. F.7).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the control information pair including a stream identifier, as taught by ITU-T, with the module of Kim et al. as modified by Zhang et al.

It would have been obvious for such modifications because a stream identifier would identify the elementary stream, e.g., data files. This is similar to how ECM contains a content identifier to correctly identify the content in which it refers to. The teachings of Kim et al. use ECM to identify the content, which can be transferred together with the CPTC (see col. 18, lines 61-67 of Kim et al.).

Regarding claim 19, the combination of Kim et al. as modified by Zhang et al./ITU-T teaches wherein to use the at least one control information pair in the generating of said second key the set-top box receives a transmission of said at least one control information pair, the respective copy control information of said at least one control information pair not being encrypted for the transmission (see col. 19, lines 63-67 of Kim et al., it would stand to reason that the control information is unencrypted so that it can be utilized by the host quickly).

Regarding claim 20, the combination of Kim et al. as modified by Zhang et al./ITU-T teaches wherein step b) is executed without encrypting said copy control information of said at least one control information pair (see col. 19, lines 63-67 of Kim et al.).

Regarding claim 21, the combination of Kim et al. as modified by Zhang et al./ITU-T teaches wherein said copy control information of said at least one control



information pair in the reply message is unencrypted upon transmission to the host device (see 19, lines 63-67 of Kim et al.).

Regarding claim 22, the combination of Kim et al. as modified by Zhang et al./ITU-T teaches wherein the information to be encrypted comprises content information (see col. 10, lines 22-25 of Zhang et al.).

Regarding claim 23, the combination of Kim et al. as modified by Zhang et al./ITU-T teaches wherein said content information comprises content information of an elementary stream, said stream identifier being an identifier of an elementary stream (see fig. 4, step num 9 of Zhang et al. and page xi, section intro. 8.1 of ITU-T).

Regarding claims 24 and 27, the combination of Kim et al. as modified by Zhang et al./ITU-T teaches wherein said stream identifier uniquely identifies an elementary stream that is assigned said copy control information (see Intro 2, page ix, Intro 4, page x, Fig. F2, and Fig. F7 of ITU-T, the program stream and PES, containing a stream ID, while in combination with the CW and CP of Kim et al. (fig. 21) will identify the copy control information uniquely assigned with the stream identifier).

Regarding claims 25 and 28, the combination of Kim et al. as modified by Zhang et al./ITU-T teaches wherein said stream identifier is within a Packetized Elementary

Stream (PES) header of the elementary stream (see fig. F2 and F7 of ITU-T, the stream ID (F2) is contained within the PES header (F7)).

Regarding claims 26 and 29, the combination of Kim et al. as modified by Zhang et al./ITU-T teaches wherein the encrypted information to be transmitted to the set-top box includes said header, said set-top box being configured to retrieve said stream identifier from said header (see fig. 21, ref. num 263 of Kim et al., uses CW to decrypt the information. The CW as combined with fig. F2 & F7 ITU-T contains the stream ID contained in the header).

#### ***Response to Arguments***

4. Applicant argues the stream ID of ITU-T is not uniquely identified with a particular elementary stream and identifies a CCI assigned to a particular elementary stream (page 9 and top of page 10).

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., the stream identifier to uniquely identify the CCI that it is paired with) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The original claims never claimed the stream identifier being coupled and identifying a CCI that it is

Art Unit: 2136

assigned to. The claim merely cited a control information pair, containing a CCI and a stream identifier. Claiming two items are contained in a pair does not imply that one of those items uniquely identifies the other item. Accordingly, the argument is not persuasive.

### ***Conclusion***

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

Art Unit: 2136

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

*Branda Hoff*

BH

*Cell*  
Primary Examiner  
AU2131  
8/12/05